

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-108205

(43)Date of publication of application : 10.04.2002

(51)Int.Cl.

G09C 1/00

(21)Application number : 2000-295520

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

(22)Date of filing : 28.09.2000

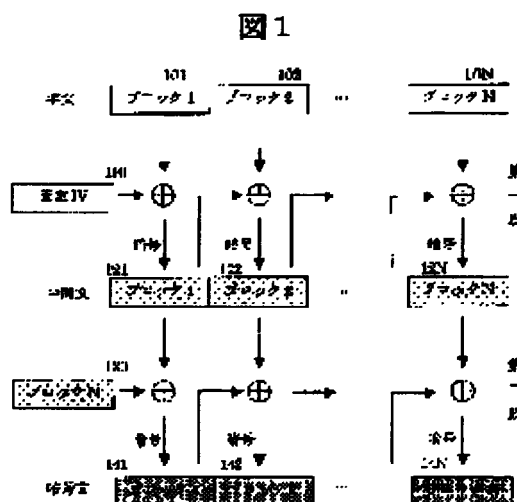
(72)Inventor : SAMEJIMA YOSHIKI

(54) BLOCK CIPHERING METHOD AND DECODING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a block ciphering method and a decoding method by which the original data can hardly be guessed at the time of making large data into a block and ciphering them.

SOLUTION: The ciphering stage of input data is constituted of at least two stages. Data is ciphered by using a password sentence block link mode in the block unit of prescribed byte length in the respective ciphering stages. In the initial ciphering stage, a fixed initialization vector which does not depend on input data is used and the ciphering result of one block in the previous ciphering stage is used as the initialization vector in the next and subsequent ciphering stages.



LEGAL STATUS

[Date of request for examination] 08.10.2002

[Date of sending the examiner's decision of rejection] 13.12.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-108205
(P2002-108205A)

(43) 公開日 平成14年4月10日 (2002.4.10)

(51) Int.Cl.⁷
G 0 9 C 1/00

識別記号
6 1 0

F I
G 0 9 C 1/00

データベース* (参考)
6 1 0 A 5 J 1 0 4

審査請求 未請求 請求項の数 4 O L (全 4 頁)

(21) 出願番号 特願2000-295520 (P2000-295520)

(22) 出願日 平成12年9月28日 (2000.9.28)

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会
社

神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 鮫島 吉喜

神奈川県横浜市中区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内

(74) 代理人 100088720

弁理士 小川 真一

Fターム (参考) 5J104 AA16 EA04 JA03 NA02 NA04

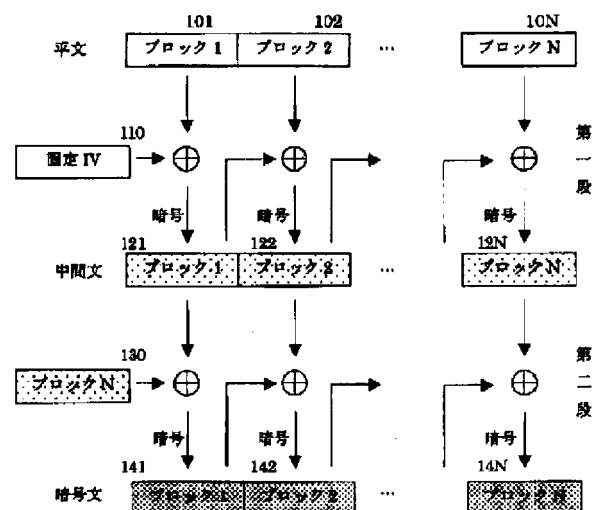
(54) 【発明の名称】 ブロック暗号方法及び復号方法

(57) 【要約】

【課題】 大きなデータをブロック化して暗号化する際に、元のデータが推測されるのを困難にすることができるブロック暗号方法及び復号方法を提供すること。

【解決手段】 入力データの暗号化段階を少なくとも2つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における1つのブロックの暗号結果を初期化ベクトルとして用いる。

図 1



【特許請求の範囲】

【請求項 1】 入力データを所定バイト長のブロック単位で暗号化するブロック暗号方法において、入力データの暗号化段階を少なくとも 2 つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における 1 つのブロックの暗号結果を初期化ベクトルとして用いることを特徴とするブロック暗号方法。

【請求項 2】 前記最初の暗号化段階以降に用いる初期化ベクトルとして、前の暗号化段階における最後のブロックの暗号結果を用いることを特徴とする請求項 1 に記載のブロック暗号方法。

【請求項 3】 所定バイト長のブロック単位で暗号化されたデータを復号するブロック暗号復号方法において、復号対象の入力データの復号段階を少なくとも 2 つの段階で構成し、かつ最後の暗号化段階から最初の暗号化段階に向かう順で復号し、最初の復号段階から最後の復号段階の 1 つ前までの復号段階では次に行う復号段階における 1 つのブロックの暗号結果を初期化ベクトルとして用い、最後の復号段階では固定の初期化ベクトルを用いることを特徴とするブロック暗号復号方法。

【請求項 4】 前記最初の復号段階から最後の復号段階の 1 つ前までの復号段階で用いる初期化ベクトルとして、次の復号段階における大ブロック内の最後のブロックの暗号結果を用いることを特徴とする請求項 3 に記載のブロック暗号復号方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ブロック暗号方法および復号方法に関するものである。

【0002】

【従来の技術】 既存の秘密鍵暗号の暗号単位は、8 バイト程度と比較的小さい。512 バイト程度の大きなデータを暗号化する場合には、一般に CBC モード (cipher block chaining モード; 暗号文ブロック連鎖) といわれる方法で暗号化している。図 4 にその概要を示す。

【0003】 図 4 において、暗号化対象の平文 (入力データ) は、例えば 8 バイト単位のブロック 1 (401) ~ N (40N) に分割される。平文のブロック 1 (401) を暗号化するには、ブロック 1 (401) と初期化ベクタ (IV) と呼ばれるパラメータとの排他的論理和を暗号化し、暗号化されたブロック 1 (421) を得る。次に、平文のブロック 2 (402) を暗号化するが、この場合には、暗号化したブロック 1 (421) とブロック 2 (402) との排他的論理和を暗号化する。以下これを繰り返す。ブロック N (40N) を暗号化するには、暗号化したブロック N-1 と平文のブロック N (40N) との排他的論理和を暗号化する。

【0004】

【発明が解決しようとする課題】 CBC モードでは、大きなデータの最初のブロックがいくつか同じであれば、暗号文の最初のいくつかのブロックも同じになってしまう。元のデータが推測され、解読される可能性が大きくなる。例えば、データ A とデータ B とでブロック 1、ブロック 2 が同じであり、ブロック 3 が異なっていた場合、暗号文のブロック 1 とブロック 2 が同じになってしまう。

10 【0005】 本発明は、大きなデータをブロック化して暗号化する際に、元のデータが推測されるのを困難にすることができるブロック暗号方法及び復号方法を提供することにある。

【0006】

【課題を解決するための手段】 上記課題を解決するために、本発明のブロック暗号方法は、入力データの暗号化段階を少なくとも 2 つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における 1 つのブロックの暗号結果を初期化ベクトルとして用いることを特徴とする。

【0007】 また、前記最初の暗号化段階以降に用いる初期化ベクトルとして、前の暗号化段階における最後のブロックの暗号結果を用いることを特徴とする。

【0008】 また、本発明のブロック暗号復号方法は、所定バイト長のブロック単位で暗号化されたデータを復号するブロック暗号復号方法において、復号対象の入力データの復号段階を少なくとも 2 つの段階で構成し、かつ最後の暗号化段階から最初の暗号化段階に向かう順で復号し、最初の復号段階から最後の復号段階の 1 つ前までの復号段階では次に行う復号段階における 1 つのブロックの暗号結果を初期化ベクトルとして用い、最後の復号段階では固定の初期化ベクトルを用いることを特徴とする。

【0009】 また、前記最初の復号段階から最後の復号段階の 1 つ前までの復号段階で用いる初期化ベクトルとして、次の復号段階における大ブロック内の最後のブロックの暗号結果を用いることを特徴とする。

【0010】

【発明の実施の形態】 以下、本発明を図示する実施形態に従い詳細に説明する。図 1 は、本発明のブロック暗号方法の概要を示す図である。本発明では、入力データの暗号化段階を少なくとも 2 つの段階で構成し、各暗号化段階で前記所定バイト長のブロック単位で暗号文ブロック連鎖モードを用いて暗号化し、かつ最初の暗号化段階では入力データに依存しない固定の初期化ベクトルを用い、次の暗号化段階以降では前の暗号化段階における 1 つのブロックの暗号結果を初期化ベクトルとして用い

る。

【0011】図1の例では、説明を簡単にするために、暗号化段階を2段階にした例を示している。そして、最初の暗号化段階以降（2段階目の暗号化段階）に用いる初期化ベクトルとして、前の暗号化段階（最初の暗号化段階）における大ブロック内の最後のブロックNの暗号結果を用いる例を示している。この場合、最後のブロックNの暗号結果を用いる代わりに、ブロックNの暗号結果を基に生成した初期化ベクトル、あるいは他のブロックの暗号結果を用いることもできる。ただし、最後のブ

【0012】図1において、101～10Nは、平文のブロック1からブロックN、110は固定の初期化ベクトル(1V)を示す。この1V(110)は固定にしてもよいし、システム全体で固定してもよい。121～12Nは、中間文のブロック1～ブロックN、130はブロックN(12N)と同一であり、二段目の暗号化段階で使用する初期化ベクトルとなる。141～14Nまでは、暗号文のブロック1からブロックNである。

【0013】図1で示す暗号化方法は、2段階の暗号化段階からなり、途中で中間文のブロック1(121)～ブロックN(12N)を生成する。ブロック1(101)～ブロックN(10N)から成る平文を暗号して中間文を生成するには、平文に依存しない固定の初期化ベクトル(110)を用いて先に説明したCBCモードを用いて暗号化する。次に、中間文を、その中間文のブロックN(12N)を初期化ベクトル(130)として用い、CBCモードで暗号化して、ブロック1(141)～ブロックN(14N)から成る最終の暗号文を得る。なお、ここで、最初の秘密鍵暗号と次の秘密鍵暗号の方法は異なってもよい。

【0014】図2に、図1で説明した暗号化方法の処理手順をフローチャートにより示している。本発明のブロック暗号方法及び復号方法は、特に図示しないが、コンピュータとそのハードウェア資源を用いて実施するものである。図2において、まず、ステップ201で固定の初期化ベクトル(110)を用い、ブロック1(101)～ブロックN(10N)から成る平文をCBCモードで第一段の秘密鍵暗号にしたがって暗号化し、ブロック1(121)～ブロックN(12N)から成る中間文を得る。すなわち、ブロック1(101)と固定の初期化ベクトル(110)の排他的論理和を暗号化して中間文のブロック1(121)を得る。次に平文のブロック(102)と中間文のブロック1(121)の排他的論理和を第一段の秘密鍵暗号にしたがって暗号化し、中間文のブロック2(122)を得る。以下これを繰り返

し、中間文のブロックN(12N)を得る。

【0015】次に、ステップ202において、中間文のブロックN(12N)を初期化ベクトル(130)として用い、ブロック1(121)～ブロックN(12N)

から成る中間文をCBCモードで第二段の秘密鍵暗号にしたがって暗号化し、最終の暗号文を得る。すなわち、中間文のブロック1(121)と初期化ベクトル(130)の排他的論理和を第二段の秘密鍵暗号にしたがって暗号化して最終の暗号文のブロック1(141)を得る。次に、中間文のブロック2(122)と最終の暗号文のブロック1(141)の排他的論理和を第二段の秘密鍵暗号にしたがって暗号化してブロック2(142)を得る。以下これを繰り返し、最終の暗号文のブロックN(14N)を得る。

【0016】次に、図3のフローチャートを用いて復号処理について説明する。まずステップ301において、最終の暗号文のブロックN(14N)を第二段の秘密鍵暗号にしたがって復号し、中間文のブロックN(12N)を得る。

【0017】次にステップ302において、ブロックN(12N)と同一の初期化ベクトル(130)を用い、最終の暗号文をCBCモードで第二段の秘密鍵暗号にしたがって復号し、中間文を得る。すなわち、ブロック(141)を第二段の秘密鍵暗号にしたがって復号し、初期化ベクトル(130)との排他的論理和をとり、ブロック1(121)を得る。次に、ブロック2(142)を第二段の秘密鍵暗号にしたがって復号し、ブロック(141)との排他的論理和をとり、ブロック(122)を得る。以下これを繰り返し、ブロック1(121)～ブロックN(12N)から成る中間文を得る。

【0018】次に、ステップ303において、固定の初期化ベクトル(110)を用い、中間文をCBCモードで第一段の秘密鍵暗号にしたがって復号し、ブロック1(101)～ブロックN(10N)から成る平文を得る。すなわち、ブロック(121)を第一段の秘密鍵暗号にしたがって復号し、ブロック(110)との排他的論理和をとり、ブロック(101)を得る。次に、ブロック(122)を第一段の秘密鍵暗号にしたがって復号し、ブロック(121)の排他的論理和をとり、ブロック(102)を得る。以下これを繰り返し、ブロック(10N)を得、最終の平文を得る。

【0019】

【発明の効果】以上説明した本発明によれば、例えば512バイト長などの比較的大きなデータを安全に暗号化することができる。すなわち、512バイト長などの比較的大きなデータでは、最初のブロックに同じデータが存在することがあるが、本発明によれば、第二段の暗号化段階で平文に応じて異なる初期化ベクトルを用いて暗号化するので、異なる暗号文を得ることができ、解読を困難にすることができる。

【図面の簡単な説明】

【図1】本発明のブロック暗号方法の概要を示す図である。

【図2】本発明のブロック暗号方法の処理手順を示すフ

ローチャートである。

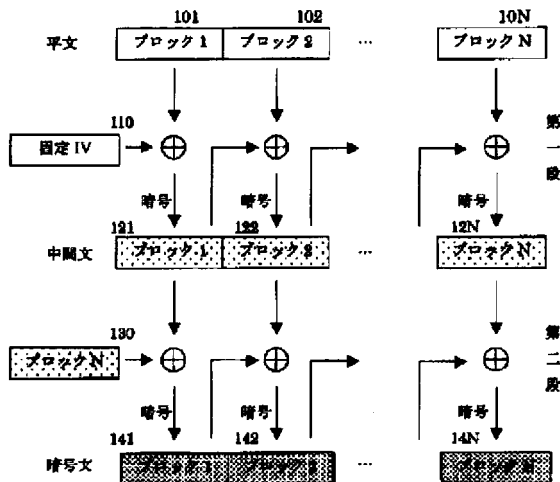
【図 3】 本発明のブロック暗号復号方法の処理手順を示すフローチャートである。

【図 4】 従来のブロック暗号方法の概要を示す図である。

*

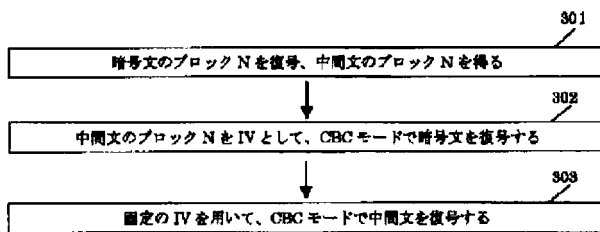
【図 1】

図 1



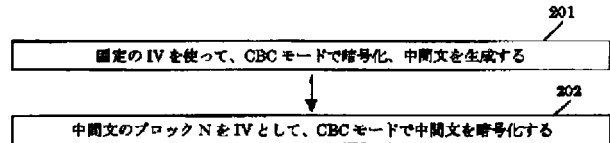
【図 3】

図 3



【図 2】

図 2



【図 4】

図 4

